PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-033727
(43)Date of publication of application : 31.01.2002

(51)Int.Cl. H04L 9/10
G06F 12/00
G06F 12/14
H04L 9/08
H04L 9/32

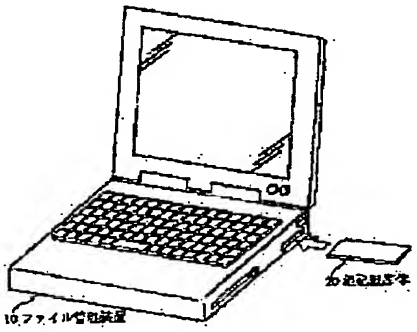
(21)Application number : 2001-137650
(22)Date of filing : 08.05.2001

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
EMURA SATOSHI
INAGAKI SATORU

(30)Priority
Priority number : 2000138642 Priority date : 11.05.2000 Priority country : JP

(54) FILE MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a file management system that can surely decode encrypted information, when a user forgets a password.
SOLUTION: A password registration section 100 uses a password, to encrypt key information and to store an encrypted key. A file encryption section 200 uses the key information to encrypt a file key and to generate an encrypted file key, uses the file key to encrypt a plain text and generates an encrypted text to store the encrypted file key and the encrypt text. A file decoding section 300 decodes the encrypted file key, by using the key information to obtain a file key, when using the key information. When using the password, the password is received, the encryption key is decoded by the password to obtain the key information, the file key is decoded by using the encrypted file key to obtain the file key. Then the encrypted text is decoded by the file key.



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－33727
（P2002－33727A）
(43)公開日　平成14年１月31日(2002.1.31)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04L	9/10		G06F	12/00	537H 5B017
G06F	12/00	537		12/14	320B 5B082
	12/14	320			320C 5J104
			H04L	9/00	621A
H04L	9/08				673C

審査請求　未請求　請求項の数37　ＯＬ　（全 24 頁）　最終頁に続く

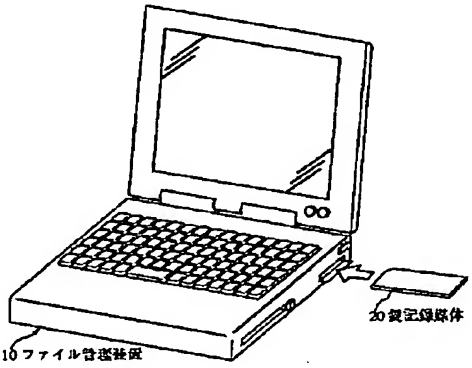
(21)出願番号　特願2001－137650(P2001－137650)
(22)出願日　平成13年５月８日(2001.5.8)
(31)優先権主張番号　特願2000－138642(P2000－138642)
(32)優先日　平成12年５月11日(2000.5.11)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業　株式会社内
(72)発明者　江村　里志
大阪府門真市大字門真1006番地　松下電器産業　株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　ファイル管理装置

(57)【要約】
【課題】　利用者がパスワードを忘れたとき、暗号化された情報が確実に復号できるファイル管理装置を提供する。
【解決手段】　パスワード登録部１００はパスワードを用いて鍵情報を暗号化し暗号化鍵を保存する。ファイル暗号部２００は鍵情報を用いてファイル鍵を暗号化して暗号化ファイル鍵を生成しファイル鍵を用いて平文を暗号化して暗号文を生成し暗号化ファイル鍵と暗号文とを保存する。鍵情報を用いるときファイル復号部３００は暗号化ファイル鍵を鍵情報を用いて復号してファイル鍵を求める。パスワードを用いるときパスワードを受け付け暗号化鍵をパスワードで復号して鍵情報を求め鍵情報で暗号化ファイル鍵を復号してファイル鍵を求める。次にファイル鍵で暗号文を復号する。



1

【特許請求の範囲】

【請求項１】 平文を暗号化して記憶し、復号するファイル管理装置であって、

鍵情報を予め記憶している鍵記録媒体と、

入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、

前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、

前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切換手段と、

前記鍵情報に基づいて暗号文を復号する復号手段とを備えることを特徴とするファイル管理装置。

【請求項２】 前記ファイル管理装置は、さらにメモリ部を有し、

前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、

前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、

前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第１鍵獲得手段と、第２タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第２鍵獲得手段とを含み、前記切換手段は、前記第１及び第２鍵獲得手段のいずれかにより鍵情報を獲得し、

前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成することを特徴とする請求項１に記載のファイル管理装置。

【請求項３】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化鍵をメモリ部に書き込み、

前記第１鍵獲得手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化鍵を復号することを特徴とする請求項２に記載のファイル管理装置。

【請求項４】 前記登録手段は、さらに前記鍵情報又は認証情報を前記暗号化鍵と対応付けてメモリ部に書き込み、

前記暗号手段は、さらに前記暗号化鍵、前記鍵情報又は認証情報を前記暗号文と対応付けてメモリ部に書き込み、

前記第１鍵獲得手段は、さらに前記認証情報が対応付けられた前記暗号化鍵を復号する場合に、前記認証情報を用いて前記暗号化鍵の改竄の有無を検証し、

前記復号手段は、さらに前記認証情報が対応付けられた

2

前記暗号文を復号する場合に、前記認証情報を用いて前記暗号文の改竄の有無を検証することを特徴とする請求項２に記載のファイル管理装置。

【請求項５】 前記登録手段は、前記暗号化鍵を可搬型記録媒体であるメモリ部に書き込み、

前記第１鍵獲得手段は、前記可搬型記録媒体であるメモリ部に書き込まれている前記暗号化鍵を復号することを特徴とする請求項２に記載のファイル管理装置。

【請求項６】 前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含むことを特徴とする請求項２に記載のファイル管理装置。

【請求項７】 前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含み、

前記登録手段は、さらに、新パスワードの入力を受け付け、前記新パスワードを用いて前記鍵情報を暗号化して新暗号化鍵を生成し、生成した前記新暗号化鍵をメモリ部に書き込むことを特徴とする請求項２に記載のファイル管理装置。

【請求項８】 前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、

前記登録手段は、さらに前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成し、

前記暗号手段は、さらに前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新暗号化ファイル鍵を生成し、前記暗号化ファイル鍵に代えて前記新暗号化ファイル鍵をメモリ部に書き込み、

前記登録手段は、さらに前記パスワードを用いて前記新鍵情報を暗号化して新暗号化鍵を生成し、前記暗号化鍵に代えて生成した前記新暗号化鍵をメモリ部に書き込むことを特徴とする請求項２に記載のファイル管理装置。

【請求項９】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、メモリ部内において前記利用者識別子に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項８に記載のファイル管理装置。

【請求項１０】 前記暗号手段は、さらに暗号化を示す暗号化情報を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、メモリ部内において暗号化情報に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項８に記載のファイル管理装置。

【請求項１１】 前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、
前記暗号手段は、さらに前記利用者識別子と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、
前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項８に記載のファイル管理装置。

【請求項１２】 前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、
前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成することを特徴とする請求項８に記載のファイル管理装置。

【請求項１３】 前記暗号手段は、さらに前記暗号化鍵を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、
前記第１鍵獲得手段は、前記暗号文及び前記暗号化ファイル鍵と対応付けて記憶されている前記暗号化鍵を復号することを特徴とする請求項２に記載のファイル管理装置。

【請求項１４】 前記暗号手段は、さらに、暗号化鍵と暗号文とを対応付けてメモリ部に書き込むか否かを示す指示の入力を受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵を前記暗号文と対応付けてメモリ部に書き込むことを特徴とする請求項１３に記載のファイル管理装置。

【請求項１５】 前記登録手段は、生成した前記暗号化鍵を、メモリ部に代えて、前記鍵記録媒体に書き込むことを特徴とする請求項１３に記載のファイル管理装置。

【請求項１６】 平文を暗号化してメモリ部に記憶するファイル暗号装置であって、
鍵情報を予め記憶している鍵記録媒体と、
パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込む登録手段と、
ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とするファイル暗号装置。

【請求項１７】 請求項１６に記載のファイル暗号装置

により生成された前記暗号文と前記暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、
鍵情報を予め記憶している鍵記録媒体と、
前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第１鍵獲得手段と、前記鍵記録媒体から鍵情報を読み出す第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかにより鍵情報を獲得する切換手段と、
前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とするファイル復号装置。

【請求項１８】 平文を暗号化して記憶し、復号するファイル管理装置であって、
鍵情報を予め記憶している鍵記録媒体と、
前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、
ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、
前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切換手段と、
前記ファイル鍵に基づいて暗号文を復号する復号手段とを備えることを特徴とするファイル管理装置。

【請求項１９】 前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、
前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、
前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第１暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第２暗号化ファイル鍵を生成し、前記暗号文と前記第１及び第２暗号化ファイル鍵とを対応付けてメモリ部に書き込み、
前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成する第１鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成する第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかによりファイル鍵を獲得し、
前記復号手段は、前記ファイル鍵を用いて前記暗号文を

復号して復号文を生成することを特徴とする請求項１８に記載のファイル管理装置。

【請求項２０】　前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化パスワードを復号することを特徴とする請求項１９に記載のファイル管理装置。

【請求項２１】　前記暗号手段は、前記第１暗号化ファイル鍵を生成するか否かを示す指示を受け付け、生成する旨の指示を受け付けた場合に、前記第１暗号化ファイル鍵を生成し、生成しない旨の指示を受け付けた場合に、前記第１暗号化ファイル鍵の生成と、前記第１暗号化ファイル鍵の書き込みとを抑制することを特徴とする請求項１９に記載のファイル管理装置。

【請求項２２】　前記登録手段は、さらに認証情報を前記暗号化パスワードと対応付けてメモリ部に書き込み、

前記暗号手段は、さらに前記暗号化パスワードを復号する場合に、前記認証情報を用いて前記暗号化パスワードの改竄の有無を検証し、

前記暗号手段は、さらに第１暗号化ファイル鍵、第２暗号化ファイル鍵及び暗号文のそれぞれに、対応する認証情報を対応づけてメモリ部に書き込み、

前記第１及び第２鍵獲得手段は、さらに第１暗号化ファイル鍵及び第２暗号化ファイル鍵を復号する場合に、それぞれ対応付けられた前記認証情報を用いて改竄の有無を検証し、

前記復号手段は、さらに暗号文を復号する場合に、対応付けられた前記認証情報を用いて改竄の有無を検証することを特徴とする請求項１９に記載のファイル管理装置。

【請求項２３】　前記登録手段は、前記暗号化パスワードを、前記メモリ部に代えて、前記鍵記録媒体に書き込み、

前記暗号手段は、前記鍵記録媒体に書き込まれている前記暗号化パスワードを復号することを特徴とする請求項１９に記載のファイル管理装置。

【請求項２４】　前記登録手段は、さらに新パスワードの入力を受け付け、前記鍵情報を用いて前記新パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、さらに前記鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成し、前記新パスワードを用いて前記ファイル鍵を暗号化して新第１暗号化ファイル鍵を生成し、前記第１暗号化ファイル鍵に代えて、前記新第１暗号化ファイル鍵をメモリ部に書き込むことを特徴とする請求項１９に記載のファイル管理装置。

【請求項２５】　前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記利用者識別子に対応づけられた前記第２暗号化ファイル鍵を検索し、検索した前記第２暗号化ファイル鍵を復号することを特徴とする請求項２４に記載のファイル管理装置。

【請求項２６】　前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記暗号化情報が対応づけられた前記第２暗号化ファイル鍵を検索し、検索した前記第２暗号化ファイル鍵を復号することを特徴とする請求項２４に記載のファイル管理装置。

【請求項２７】　前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第２暗号化ファイル鍵を特定し、特定された前記第２暗号化ファイル鍵を復号することを特徴とする請求項２４に記載のファイル管理装置。

【請求項２８】　前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第２暗号化ファイル鍵を特定し、特定された前記第２暗号化ファイル鍵を復号することを特徴とする請求項２４に記載のファイル管理装置。

【請求項２９】　前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記第２暗号化ファイル鍵を削除する削除手段を含むことを特徴とする請求項１９に記載のファイル管理装置。

【請求項３０】　前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、

前記登録手段は、前記パスワードの入力を受け付け、前記新鍵情報を用いて前記パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代え

て、生成した前記新暗号化パスワードをメモリ部に書き込み、

前記暗号手段は、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新第２暗号化ファイル鍵を生成し、前記第２暗号化ファイル鍵に代えて、前記新第２暗号化ファイル鍵を前記メモリ部に書き込むことを特徴とする請求項１９に記載のファイル管理装置。

【請求項３１】　前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記利用者識別子に対応づけらけた前記第１暗号化ファイル鍵を検索し、検索した前記第１暗号化ファイル鍵を復号することを特徴とする請求項３０に記載のファイル管理装置。

【請求項３２】　前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、

前記暗号手段は、前記暗号化情報が対応づけらけた前記第１暗号化ファイル鍵を検索し、検索した前記第１暗号化ファイル鍵を復号することを特徴とする請求項３０に記載のファイル管理装置。

【請求項３３】　前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、

前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけらけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第１暗号化ファイル鍵を特定し、特定された前記第１暗号化ファイル鍵を復号することを特徴とする請求項３０に記載のファイル管理装置。

【請求項３４】　前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、

前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけらけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第１暗号化ファイル鍵を特定し、特定された前記第１暗号化ファイル鍵を復号することを特徴とする請求項３０に記載のファイル管理装置。

【請求項３５】　前記切換手段は、さらに、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号して第１ファイル鍵を生成し、前記鍵情報を用いて前記第２暗号化ファイル鍵を復号して第２ファイル鍵を生成し、前記第１ファイル鍵と前記第２ファイル鍵とが一致するか否かを判断し、一致しない場合に、エラーとすることを特徴とする請求項１９に記載のファイル管理装置。

【請求項３６】　平文を暗号化してメモリ部に記憶するファイル暗号装置であって、

鍵情報を予め記憶している鍵記録媒体と、

パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込む登録手段と、

前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第１暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第２暗号化ファイル鍵を生成し、前記暗号文と前記第１及び第２暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とするファイル暗号装置。

【請求項３７】　請求項３５のファイル暗号装置により生成された前記暗号文と前記第１暗号化ファイル鍵と前記第２暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、

鍵情報を予め記憶している鍵記録媒体と、

前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成する第１鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成する第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかによりファイル鍵を獲得する切換手段と、

前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とするファイル復号装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報を暗号化して記憶し、第三者への情報漏洩を防止するファイル管理装置に関する。

【０００２】

【従来の技術】コンピュータの普及に伴い、情報が第三者へ漏洩しないように、情報を暗号化して記憶する技術が一般に用いられるようになってきている。特開平９－２０４３３０号公報により開示されている技術によると、計算機内のファイルがある暗号鍵を用いて暗号化されて特定の暗号情報格納領域に格納され、特定の利用者

のみが前記暗号情報格納領域にアクセスできるように、認証パスワードが登録され、前記利用者は、前記認証パスワードを記憶しておく。前記利用者が、記憶している前記認証パスワードを入力すると、復号鍵が自動的に選ばれて暗号化されたファイルが復号される。ここで、前記認証パスワードは、人が記憶できる程度に短い文字列や数字であり、前記暗号鍵、又は前記復号鍵は、前記認証パスワードと比べて長いビット数のものである。

【０００３】

【発明が解決しようとする課題】しかしながら、利用者は、前記認証パスワードを覚えておかなければならず、利用者が前記認証パスワードを忘れてしまった場合には、暗号化された情報が復号できないという問題点がある。上記の問題点を解決するために、本発明は、暗号化された情報を安全に管理でき、さらに利用者がパスワードを忘れた場合であっても、暗号化された情報が確実に復号できるファイル管理装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】上記目的を達成するために、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切換手段と、前記鍵情報に基づいて暗号文を復号する復号手段とを備えることを特徴する。

【０００５】ここで、前記ファイル管理装置は、さらにメモリ部を有し、前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第１鍵獲得手段と、第２タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第２鍵獲得手段とを含み、前記切換手段は、前記第１及び第２鍵獲得手段のいずれかにより鍵情報を獲得し、前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【０００６】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化鍵をメモリ部に書き込み、前記第１鍵獲得手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化鍵を復号するように構成してもよい。ここで、前記登録手段は、さらに前記鍵情報又は認証情報を前記暗号化鍵と対応付けてメモリ部に書き込み、前記暗号手段は、さらに前記暗号化鍵、前記鍵情報又は認証情報を前記暗号文と対応付けてメモリ部に書き込み、前記第１鍵獲得手段は、さらに前記認証情報が対応付けられた前記暗号化鍵を復号する場合に、前記認証情報を用いて前記暗号化鍵の改竄の有無を検証し、前記復号手段は、さらに前記認証情報が対応付けられた前記暗号文を復号する場合に、前記認証情報を用いて前記暗号文の改竄の有無を検証するように構成してもよい。

【０００７】ここで、前記登録手段は、前記暗号化鍵を可搬型記録媒体であるメモリ部に書き込み、前記第１鍵獲得手段は、前記可搬型記録媒体であるメモリ部に書き込まれている前記暗号化鍵を復号するように構成してもよい。ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含むように構成してもよい。

【０００８】ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記暗号化鍵を削除する削除手段を含み、前記登録手段は、さらに、新パスワードの入力を受け付け、前記新パスワードを用いて前記鍵情報を暗号化して新暗号化鍵を生成し、生成した前記新暗号化鍵をメモリ部に書き込むように構成してもよい。

【０００９】ここで、前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、前記登録手段は、さらに前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成し、前記暗号手段は、さらに前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新暗号化ファイル鍵を生成し、前記暗号化ファイル鍵に代えて前記新暗号化ファイル鍵をメモリ部に書き込み、前記登録手段は、さらに前記パスワードを用いて前記新鍵情報を暗号化して新暗号化鍵を生成し、前記暗号化鍵に代えて生成した前記新暗号化鍵をメモリ部に書き込むように構成してもよい。

【００１０】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、メモリ部内において前記利用者識別子に対応づけられた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【００１１】ここで、前記暗号手段は、さらに暗号化を

示す暗号化情報を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、メモリ部内において暗号化情報に対応づけらけた前記暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけらけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【００１２】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけらけたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するように構成してもよい。

【００１３】ここで、前記暗号手段は、さらに前記暗号化鍵を前記暗号文及び前記暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記第１鍵獲得手段は、前記暗号文及び前記暗号化ファイル鍵と対応付けて記憶されている前記暗号化鍵を復号するように構成してもよい。ここで、前記暗号手段は、さらに、暗号化鍵と暗号文とを対応付けてメモリ部に書き込むか否かを示す指示の入力を受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵を前記暗号文と対応付けてメモリ部に書き込むように構成してもよい。

【００１４】ここで、前記登録手段は、生成した前記暗号化鍵を、メモリ部に代えて、前記鍵記録媒体に書き込むように構成してもよい。また、本発明は、平文を暗号化してメモリ部に記憶するファイル暗号装置であって、鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込む登録手段と、　ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とする。

【００１５】また、本発明は、前記ファイル暗号装置により生成された前記暗号文と前記暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復

号するファイル復号装置であって、鍵情報を予め記憶している鍵記録媒体と、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第１鍵獲得手段と、前記鍵記録媒体から鍵情報を読み出す第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかにより鍵情報を獲得する切換手段と、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【００１６】また、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切換手段と、前記ファイル鍵に基づいて暗号文を復号する復号手段とを備えることを特徴とする。

【００１７】ここで、前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第１暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第２暗号化ファイル鍵を生成し、前記暗号文と前記第１及び第２暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成する第１鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成する第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかによりファイル鍵を獲得し、前記復号手段は、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【００１８】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記利用者識別子と対応付けて前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、さらに前記利用者識別子の入力を受け付け、前記利用者識別子に対応付けられた前記暗号化パスワードを復号するように構成してもよい。こ

ここで、前記暗号手段は、前記第１暗号化ファイル鍵を生成するか否かを示す指示を受け付け、生成する旨の指示を受け付けた場合に、前記第１暗号化ファイル鍵を生成し、生成しない旨の指示を受け付けた場合に、前記第１暗号化ファイル鍵の生成と、前記第１暗号化ファイル鍵の書き込みとを抑制するように構成してもよい。

【００１９】ここで、前記登録手段は、さらに認証情報を前記暗号化パスワードと対応付けてメモリ部に書き込み、前記暗号手段は、さらに前記暗号化パスワードを復号する場合に、前記認証情報を用いて前記暗号化パスワードの改竄の有無を検証し、前記暗号手段は、さらに第１暗号化ファイル鍵、第２暗号化ファイル鍵及び暗号文のそれぞれに、対応する認証情報を対応づけてメモリ部に書き込み、前記第１及び第２鍵獲得手段は、さらに第１暗号化ファイル鍵及び第２暗号化ファイル鍵を復号する場合に、それぞれ対応付けられた前記認証情報を用いて改竄の有無を検証し、前記復号手段は、さらに暗号文を復号する場合に、対応付けられた前記認証情報を用いて改竄の有無を検証するように構成してもよい。

【００２０】ここで、前記登録手段は、前記暗号化パスワードを、前記メモリ部に代えて、前記鍵記録媒体に書き込み、前記暗号手段は、前記鍵記録媒体に書き込まれている前記暗号化パスワードを復号するように構成してもよい。ここで、前記登録手段は、さらに新パスワードの入力を受け付け、前記鍵情報を用いて前記新パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、前記暗号手段は、さらに前記鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成し、前記新パスワードを用いて前記ファイル鍵を暗号化して新第１暗号化ファイル鍵を生成し、前記第１暗号化ファイル鍵に代えて、前記新第１暗号化ファイル鍵をメモリ部に書き込むように構成してもよい。

【００２１】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記利用者識別子に対応づけられた前記第２暗号化ファイル鍵を検索し、検索した前記第２暗号化ファイル鍵を復号するように構成してもよい。

【００２２】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記暗号化情報が対応づけられた前記第２暗号化ファイル鍵を検索し、検索した前記第２暗号化ファイル鍵を復号するように構成してもよい。

【００２３】ここで、前記登録手段は、さらに利用者を

識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第２暗号化ファイル鍵を特定し、特定された前記第２暗号化ファイル鍵を復号するように構成してもよい。

【００２４】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第２暗号化ファイル鍵を特定し、特定された前記第２暗号化ファイル鍵を復号するように構成してもよい。

【００２５】ここで、前記ファイル管理装置は、さらに、メモリ部に書き込まれている前記第２暗号化ファイル鍵を削除する削除手段を含むように構成してもよい。ここで、前記鍵記録媒体は、前記鍵情報に代えて、新鍵情報を予め記憶しており、前記登録手段は、前記パスワードの入力を受け付け、前記新鍵情報を用いて前記パスワードを暗号化して新暗号化パスワードを生成し、前記暗号化パスワードに代えて、生成した前記新暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成し、前記新鍵情報を用いて前記ファイル鍵を暗号化して新第２暗号化ファイル鍵を生成し、前記第２暗号化ファイル鍵に代えて、前記新第２暗号化ファイル鍵を前記メモリ部に書き込むように構成してもよい。

【００２６】ここで、前記登録手段は、さらに利用者を識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記利用者識別子に対応づけられた前記第１暗号化ファイル鍵を検索し、検索した前記第１暗号化ファイル鍵を復号するように構成してもよい。

【００２７】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報を、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵に対応付けてメモリ部に書き込み、前記暗号手段は、前記暗号化情報が対応づけられた前記第１暗号化ファイル鍵を検索し、検索した前記第１暗号化ファイル鍵を復号するように構成してもよい。

【００２８】ここで、前記登録手段は、さらに利用者を

識別する利用者識別子の入力を受け付け、前記暗号手段は、さらに前記利用者識別子と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記利用者識別子に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第１暗号化ファイル鍵を特定し、特定された前記第１暗号化ファイル鍵を復号するように構成してもよい。

【００２９】ここで、前記暗号手段は、さらに暗号化を示す暗号化情報と、前記暗号文、前記第１暗号化ファイル鍵及び前記第２暗号化ファイル鍵を識別するファイル識別子とを対応付けて一括ファイルとしてメモリ部に書き込み、前記暗号手段は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別される前記第１暗号化ファイル鍵を特定し、特定された前記第１暗号化ファイル鍵を復号するように構成してもよい。

【００３０】ここで、前記切換手段は、さらに、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号して第１ファイル鍵を生成し、前記鍵情報を用いて前記第２暗号化ファイル鍵を復号して第２ファイル鍵を生成し、前記第１ファイル鍵と前記第２ファイル鍵とが一致するか否かを判断し、一致しない場合に、エラーとするように構成してもよい。

【００３１】また、本発明は、平文を暗号化してメモリ部に記憶するファイル暗号装置であって、鍵情報を予め記憶している鍵記録媒体と、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込む登録手段と、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第１暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第２暗号化ファイル鍵を生成し、前記暗号文と前記第１及び第２暗号化ファイル鍵とを対応付けてメモリ部に書き込む暗号手段とを備えることを特徴とする。

【００３２】また、本発明は、前記ファイル暗号装置により生成された前記暗号文と前記第１暗号化ファイル鍵と前記第２暗号化ファイル鍵とが対応付けてメモリ部に記憶されており、前記暗号文を復号するファイル復号装置であって、鍵情報を予め記憶している鍵記録媒体と、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成する第１鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成する第２鍵獲得手段とを含み、前

記第１及び第２鍵獲得手段のいずれかによりファイル鍵を獲得する切換手段と、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

【００３３】

【発明の実施の形態】１．第１の実施の形態

本発明の第１の実施の形態としてのファイル管理装置１０について説明する。ファイル管理装置１０は、図１に外観を示すように、コンピュータシステムであり、マイクロプロセッサ、ＲＯＭ、ＲＡＭ、ハードディスクユニット、ディスプレイユニット、キーボードなどから構成される。前記ＲＡＭ又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、前記装置は、その機能を達成する。ファイル管理装置１０には、鍵情報を予め記録している鍵記録媒体２０が装填される。

【００３４】１．１　ファイル管理装置１０及び鍵記録媒体２０の構成

ファイル管理装置１０及び鍵記録媒体２０の構成について説明する。ファイル管理装置１０は、図２に示すように、パスワード登録部１００、ファイル暗号部２００、ファイル復号部３００及び記憶部４００から構成されており、鍵記録媒体２０が接続される。

【００３５】パスワード登録部１００は、パスワード入力部１０１及び暗号化部１０２から構成され、ファイル暗号部２００は、ファイル鍵生成部２０１、暗号化部２０２及び暗号化部２０３から構成され、ファイル復号部３００は、パスワード入力部３０１、復号部３０２、切換部３０３、復号部３０４及び復号部３０５から構成される。

【００３６】（１）鍵記録媒体２０

鍵記録媒体２０は、不揮発性の半導体メモリにより構成される記憶領域を備える可搬性のある記録媒体であり、前記記憶領域は、５６ビット長の鍵情報を予め記憶している。鍵情報は、１人の利用者に固有の情報である。通常、前記利用者が鍵記録媒体２０を所持している。ファイル管理装置１０を使用するときに、前記利用者は、鍵記録媒体２０をファイル管理装置１０の専用の挿入口から装填し、鍵記録媒体２０をファイル管理装置１０と接続する。

【００３７】（２）記憶部４００

記憶部４００は、具体的には、ハードディスクユニットから構成され、内部に情報をファイルとして記憶する領域を備えている。各ファイルは、ファイル名により識別される。記憶部４００は、あらかじめ、平文を含む平文ファイル４０１を記憶している。

【００３８】（３）パスワード入力部１０１

パスワード入力部１０１は、利用者からパスワードの入力を受け付ける。ここで、パスワードは、８文字の数字

及び英字からなる文字列である。パスワード入力部１０１は、受け付けた前記パスワードを暗号化部１０２へ出力する。

（４）暗号化部１０２

暗号化部１０２は、パスワード入力部１０１から前記パスワードを受け取る。前記パスワードを受け取ると、暗号化部１０２は、鍵記録媒体２０の記憶領域から鍵情報を読み出し、前記パスワードが５６ビット長となるように文字列の最後に複数個の０ビットを付加し、また前記鍵情報が６４ビット長となるように前記鍵情報の最後に複数個の０ビットを付加する。次に、前記パスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムＥ１を施して、暗号化鍵を生成する。ここで、暗号アルゴリズムＥ１は、Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ（以下、ＤＥＳ）によるものである。なお、ＤＥＳについては、公知であるので説明を省略する。

【００３９】なお、図２に示すブロック図において、パスワード入力部１０１を示すブロックと暗号化部１０２を示すブロックとを結ぶ線の付近に鍵を示すマークを表示している。このマークは、暗号化部１０２において、パスワード入力部１０１からに出力されるパスワードを鍵として用いていることを示している。このことは、他の暗号化部、他の復号部についても同様である。また、後述する図１０に示すブロック図においても同様である。

【００４０】次に、暗号化部１０２は、生成した前記暗号化鍵を１個のファイルとして記憶部４００内に書き込む。

（５）ファイル鍵生成部２０１

ファイル鍵生成部２０１は、内部に乱数発生部とタイマとを備え、５６ビット長の乱数を生成し、年、月、日、時、分、秒及びミリ秒からなる現在時刻を取得し、生成した前記乱数と取得した現在時刻とに排他的論理和を施して５６ビット長のファイル鍵を生成し、生成したファイル鍵を暗号化部２０２及び暗号化部２０３へ出力する。

【００４１】（６）暗号化部２０３

暗号化部２０３は、利用者から記憶部４００に記憶されている平文ファイル４０１のファイル名の指定を受け付け、指定を受け付けたファイル名により特定される平文ファイル４０１を記憶部４００から読み出す。また、ファイル鍵生成部２０１からファイル鍵を受け取る。

【００４２】次に、暗号化部２０３は、受け取ったファイル鍵を鍵として用いて、平文ファイル４０１内に含まれる平文に暗号アルゴリズムＥ３を施して暗号文を生成する。次に、ヘッダ部とデータ部とを含むファイルであって、データ部内に生成した前記暗号文を含む暗号化ファイル４０４を記憶部４００に書き込む。ここで、暗号アルゴリズムＥ３は、ＤＥＳによるものである。

【００４３】ここで、前記平文が６４ビット長以上の場合には、暗号化部２０３は、前記平文を複数個の６４ビット長の平文ブロックに分割し、各平文ブロック毎に暗号アルゴリズムＥ３を施して暗号化ブロックを生成し、生成した複数の暗号化ブロックを結合して、暗号文とする。

（７）暗号化部２０２

暗号化部２０２は、鍵記録媒体２０から鍵情報を読み出し、ファイル鍵生成部２０１からファイル鍵を受け取り、前記ファイル鍵が６４ビット長となるように前記ファイル鍵の最後に複数個の０ビットを付加する。

【００４４】次に、暗号化部２０２は、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムＥ２を施して暗号化ファイル鍵を生成し、生成した前記暗号化ファイル鍵を、記憶部４００の暗号化ファイル４０４内のヘッダ部内に書き込む。ここで、暗号アルゴリズムＥ２は、ＤＥＳによるものである。

（８）切換部３０３

切換部３０３は、利用者から第１及び第２タイプのいずれかの入力を受け付ける。第１タイプは、パスワードを用いて暗号文を復号することを示し、第２タイプは、鍵情報を用いて暗号文を復号することを示す。

【００４５】切換部３０３は、第１タイプの入力を受け付けた場合には、復号部３０２から鍵情報を受け取り、受け取った前記鍵情報を復号部３０４へ出力する。第２タイプの入力を受け付けた場合には、鍵記録媒体２０から鍵情報を読み出し、読み出した前記鍵情報を復号部３０４へ出力する。

（９）パスワード入力部３０１

パスワード入力部３０１は、パスワード入力部１０１と同様に、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部３０２へ出力する。

【００４６】（１０）復号部３０２

復号部３０２は、パスワード入力部３０１からパスワードを受け取り、記憶部４００から暗号化鍵を読み出し、前記パスワードの長さが５６ビット長となるように、前記パスワードの最後に複数の０ビットを付加し、前記パスワードを鍵として用いて、読み出した前記暗号化鍵に復号アルゴリズムＤ１を施して鍵情報を生成する。ここで、復号アルゴリズムＤ１は、ＤＥＳによるものであり、暗号アルゴリズムＥ１の逆変換を行うアルゴリズムである。

【００４７】次に、復号部３０２は、鍵情報の先頭５６ビット長を残して、前記鍵情報から残りのビット列を削除し、５６ビット長の前記鍵情報を切換部３０３へ出力する。

（１１）復号部３０４

復号部３０４は、切換部３０３から鍵情報を受け取り、記憶部４００から暗号化ファイル４０４のヘッダ部に含まれる暗号化ファイル鍵を読み出し、受け取った前記鍵情報を鍵として用いて、読み出した暗号化ファイル鍵に

復号アルゴリズムＤ２を施してファイル鍵を生成する。ここで、復号アルゴリズムＤ２は、ＤＥＳによるものであり、暗号アルゴリズムＥ２の逆変換を行うアルゴリズムである。

【００４８】次に、復号部３０４は、生成したファイル鍵の先頭５６ビット長を残して、前記ファイル鍵から残りのビット列を削除し、５６ビット長の前記ファイル鍵を復号部３０５へ出力する。

（１２）復号部３０５

復号部３０５は、復号部３０４からファイル鍵を受け取り、記憶部４００から暗号化ファイル４０４のデータ部に含まれる暗号文を読み出し、受け取った前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成する。ここで、復号アルゴリズムＤ３は、ＤＥＳによるものであり、暗号アルゴリズムＥ３の逆変換を行うアルゴリズムである。

【００４９】ここで、前記暗号文が６４ビット長以上の場合には、復号部３０５は、前記暗号文を複数個の６４ビット長の暗号文ブロックに分割し、各暗号文ブロック毎に復号アルゴリズムＤ３を施して復号文ブロックを生成し、生成した複数の復号文ブロックを結合して、復号文とする。次に、復号部３０５は、生成した前記復号文を含む復号文ファイル４０２を記憶部４００内に書き込む。

【００５０】１．２　ファイル管理装置１０の動作

ファイル管理装置１０の動作について説明する。

（１）パスワード登録部１００の動作

パスワード登録部１００の動作について、図３に示すフローチャートを用いて説明する。

【００５１】パスワード入力部１０１は、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部１０２へ出力する（ステップＳ１０１）。次に、暗号化部１０２は、鍵記録媒体２０の記憶領域から鍵情報を読み出し（ステップＳ１０２）、前記パスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムＥ１を施して、暗号化鍵を生成し（ステップＳ１０３）、生成した前記暗号化鍵を１個のファイルとして記憶部４００内に書き込む（ステップＳ１０４）。

【００５２】（２）ファイル暗号部２００の動作

ファイル暗号部２００の動作について、図４に示すフローチャートを用いて説明する。ファイル鍵生成部２０１は、ファイル鍵を生成する（ステップＳ１２１）。次に、暗号化部２０３は、平文ファイル４０１を記憶部４００から読み出し、ファイル鍵を鍵として用いて、平文ファイル４０１内に含まれる平文に暗号アルゴリズムＥ３を施して暗号文を生成し（ステップＳ１２２）、データ部内に生成した前記暗号文を含む暗号化ファイル４０４を記憶部４００に書き込む（ステップＳ１２３）。

【００５３】次に、暗号化部２０２は、鍵記録媒体２０から鍵情報を読み出し、ファイル鍵生成部２０１からファイル鍵を受け取り、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムＥ２を施して暗号化ファイル鍵を生成し、（ステップＳ１２４）、生成した前記暗号化ファイル鍵を、記憶部４００の暗号化ファイル４０４内のヘッダ部内に書き込む（ステップＳ１２５）。

【００５４】（３）ファイル復号部３００の動作

ファイル復号部３００の動作について、図５に示すフローチャートを用いて説明する。切換部３０３は、利用者から第１及び第２タイプのいずれかの入力を受け付ける（ステップＳ１４１）。

【００５５】切換部３０３が第１タイプの入力を受け付けた場合には、（ステップＳ１４２）、パスワード入力部３０１は、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部３０２へ出力し（ステップＳ１４４）、復号部３０２は、記憶部４００から暗号化鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記暗号化鍵に復号アルゴリズムＤ１を施して鍵情報を生成し、前記鍵情報を切換部３０３を介して復号部３０４へ出力する（ステップＳ１４５）。

【００５６】切換部３０３が第２タイプの入力を受け付けた場合には（ステップＳ１４２）、切換部３０３は、鍵記録媒体２０から鍵情報を読み出し、読み出した前記鍵情報を復号部３０４へ出力する（ステップＳ１４３）。次に、復号部３０４は、切換部３０３から鍵情報を受け取り、記憶部４００から暗号化ファイル４０４のヘッダ部に含まれる暗号化ファイル鍵を読み出し、受け取った前記鍵情報を鍵として用いて、読み出した暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成し（ステップＳ１４６）、復号部３０５は、記憶部４００から暗号化ファイル４０４のデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成し（ステップＳ１４７）、次に、復号部３０５は、生成した前記復号文を含む復号文ファイル４０２を記憶部４００内に書き込む（ステップＳ１４８）。

【００５７】１．３　まとめ

以上説明したように、ファイル管理装置１０は、パスワードの登録、平文の暗号化及び暗号文の復号の３つの部分を含んでいる。パスワードの登録時には、利用者は、鍵記録媒体を装填し、登録するパスワードを入力する。パスワード登録部１００は、入力されたパスワードを用いて鍵情報を暗号化し、生成された暗号化鍵を計算機内にファイルとして保存する。

【００５８】次に、ファイルの暗号時には、利用者は、鍵記録媒体を装填し、暗号化するファイルを指定する。このとき、ファイル毎のパスワード入力が不要であるので、利用者にとって暗号化処理の操作が容易である。ファイル暗号部２００は、任意にファイル鍵を生成し、鍵情報を用いてファイル鍵を暗号化して暗号化ファイル鍵

を生成し、次にファイル鍵を用いてファイルの情報を暗号化して暗号文を生成し、そして暗号化ファイル鍵をヘッダ部に、暗号文をデータ部に含む暗号化ファイルを保存する。

【００５９】暗号文の復号には、鍵情報を用いる方法とパスワードを用いる方法とである。鍵情報を用いる場合には、ファイル復号部３００は、暗号化ファイルのヘッダ部から獲得した暗号化ファイル鍵を鍵情報を用いて復号してファイル鍵を求める。次に、暗号文をそのファイル鍵で復号する。また、パスワードを用いる場合には、パスワードの入力を受け付け、暗号化鍵をパスワードで復号して鍵情報を求め、さらに鍵情報で暗号化ファイル鍵を復号してファイル鍵を求め、最後にファイル鍵で暗号文を復号してもとの平文を求める。

【００６０】このように構成されているので、通常は、上記のように鍵情報を用いる方法を利用し、利用者が鍵情報が記録されている鍵記録媒体を持参し忘れた場合には、パスワード用いる方法により、暗号化された情報を復号することができる。

１．４　変形例

ファイル管理装置１０は、次に示すように構成してもよい。

【００６１】（１）パスワード登録部は、さらに利用者を識別する利用者識別子（利用者ＩＤ）の入力を受け付け、前記利用者ＩＤと対応付けて前記暗号化鍵をメモリ部の利用者ＩＤに書き込むようにしてもよい。図６に利用者ＩＤテーブルの一例を示す。利用者ＩＤテーブルは、利用者ＩＤと暗号化鍵とからなる組を複数個記憶する領域を備えている。このとき、ファイル復号部は、さらに前記利用者ＩＤの入力を受け付け、前記利用者ＩＤテーブルにおいて、入力された前記利用者ＩＤに対応付けられた前記暗号化鍵を復号する。

【００６２】このように構成されているので、複数の利用者によりファイル管理装置を利用することができる。

（２）パスワードを変更する場合の動作について、図７に示すフローチャートを用いて説明する。前記ファイル管理装置は、さらに、削除部を含み、前記削除部は、記憶部に書き込まれている前記暗号化鍵を削除する（ステップＳ１６１）。

【００６３】次に、パスワード登録部１００のパスワード入力部１０１は、利用者から新たなパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部１０２へ出力する（ステップＳ１６２）。次に、暗号化部１０２は、鍵記録媒体２０の記憶領域から鍵情報を読み出し（ステップＳ１６３）、前記新たなパスワードを鍵として用いて、前記鍵情報に暗号アルゴリズムＥ１を施して、新たな暗号化鍵を生成し（ステップＳ１６４）、生成した前記新たな暗号化鍵を１個のファイルとして記憶部４００内に書き込む（ステップＳ１６５）。

【００６４】このように、パスワードを更新する場合には、暗号化鍵を新たに生成すればよい。

（３）パスワードによる復号を禁止するためには、暗号化鍵を削除するだけで良い。

（４）鍵情報を更新する場合のファイル管理装置の動作について、図８に示すフローチャートを用いて説明する。

【００６５】前記鍵記録媒体は、前記鍵情報（旧鍵情報と呼ぶ）に代えて、新たな鍵情報（新鍵情報と呼ぶ）を予め記憶している。パスワード入力部１０１は、前に入力を受け付けたものと同じパスワードの入力を受け付け（ステップＳ１８１）、暗号化部１０２は、前記パスワードを用いて、前記暗号化鍵（旧暗号化鍵と呼ぶ）に復号アルゴリズムＤ１を施して旧鍵情報を生成し（ステップＳ１８２）、鍵記録媒体から新鍵情報を読み出し、前記パスワードを用いて新鍵情報に暗号アルゴリズムＥ１を施して新暗号化鍵を生成し（ステップＳ１８３）、新暗号化鍵を記憶部４００に記憶されている旧暗号化鍵に上書きする（ステップＳ１８４）。

【００６６】次に、ファイル暗号部２００は、暗号化ファイル鍵（旧暗号化ファイル鍵と呼ぶ）を読み出して、旧鍵情報を用いて旧暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成し（ステップＳ１８５）、次に、鍵記録媒体から新鍵情報を読み出し、新鍵情報を用いてファイル鍵に暗号アルゴリズムＥ２を施して新暗号化ファイル鍵を生成し（ステップＳ１８６）、次に、新暗号ファイル鍵を暗号化ファイル内の旧暗号化ファイル鍵に上書きする（ステップＳ１８７）。

【００６７】このように、鍵情報を更新する場合には、暗号化鍵とパスワードとを用いて更新前の鍵情報を一旦求めて、鍵情報を用いてヘッダにある暗号化ファイル鍵を復号してファイル鍵を求める。その後新しい鍵情報でファイル鍵を暗号化して、暗号化ファイル鍵を更新する。このとき、暗号化鍵も更新する。この実施の形態においては、鍵情報を紛失した場合に、鍵情報を一時的に無効化することはできない。

【００６８】（５）ファイル暗号部は、ファイルを暗号化するときに、暗号化ファイルのヘッダ部に、暗号化がされたか否かを示す暗号化情報を付加するようにしてもよい。このとき、鍵情報を更新する場合において、前記ファイル暗号部は、記憶部内において暗号化情報がヘッダ部に付加された暗号化ファイルから暗号化ファイル鍵を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【００６９】また、パスワード登録部は、利用者を識別する利用者ＩＤの入力を受け付け、ファイル暗号部は、さらに前記利用者ＩＤを、前記暗号文及び前記暗号化ファイル鍵を含む暗号化ファイル内に付加して書き込むようにしてもよい。このとき、鍵情報を更新する場合において、ファイル暗号部は、記憶部内において前記利用者ＩＤが付加された暗号化ファイル内の暗号化ファイル鍵

を検索し、検索された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【００７０】また、ファイル暗号化部は、前記利用者ＩＤと、前記暗号文及び前記暗号化ファイル鍵を含む暗号化ファイルを識別するファイル識別子とを対応付けて一括ファイルとして記憶部に書き込むとしてもよい。このとき、ファイル暗号化部は、前記一括ファイルから前記利用者ＩＤに対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別されるファイルに含まれる暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するようにしてもよい。

【００７１】また、ファイル暗号化部は、暗号化を示す暗号化情報と、前記暗号文及び前記暗号化ファイル鍵を含むファイルを識別するファイル識別子とを対応付けて一括ファイルとして記憶部に書き込むようにしてもよい。このとき、ファイル暗号化部は、前記一括ファイルから前記暗号化情報に対応づけられたファイル識別子を抽出し、抽出されたファイル識別子により識別されるファイルに含まれる暗号化ファイル鍵を特定し、特定された前記暗号化ファイル鍵からファイル鍵を生成するとしてもよい。

【００７２】（６）上記の実施の形態では、暗号化鍵は、当該ファイルを暗号化したコンピュータシステム内に保存されているので、パスワードによる暗号文の復号は、当該コンピュータシステム内でのみ可能となる。ここで、他のコンピュータシステムにおいて、パスワードによる復号を可能にするためには、暗号化鍵を可搬型の別記録媒体に格納し、他のコンピュータシステムに入力すればよい。

【００７３】ここで、１個のコンピュータシステムのパスワード登録部は、ＳＤメモリカードなどの可搬型の記録媒体に暗号化鍵を書き込む。また、利用者は、暗号化ファイルを可搬型の記録媒体に書き込む。次に、利用者は、暗号化鍵の書き込まれた記録媒体と、暗号化ファイルの書き込まれた記録媒体を他のコンピュータシステムに装填し、他のコンピュータシステムが備えるファイル復号部は、可搬型記録媒体から暗号化鍵を読み出し、復号し、また可搬型記録媒体から暗号文を読み出し、復号する。

【００７４】ここで、暗号化鍵と暗号文とを別のファイルにして、１個の可搬型の記録媒体に書き込むとしてもよい。

（７）パスワード登録部は、鍵記録媒体２０から鍵情報を読み出し、読み出した鍵情報にハッシュアルゴリズムを施して第１認証情報を生成し、生成した第１認証情報を前記暗号鍵と対応付けて、記憶部４００に書き込ようにしてもよい。このとき、ファイル復号部は、暗号化鍵と第１認証情報とを記憶部から読み出し、暗号化鍵を復号して鍵情報を生成し、生成した前記鍵情報に、上記と

同じハッシュアルゴリズムを施して、第２認証情報を生成する。次に、ファイル復号部は、第１認証情報と第２認証情報とを比較して同一でなければ、暗号化鍵が改竄されたものと判断し、同一であれば、暗号化鍵が改竄されていないものと判断する。

【００７５】ファイル暗号部は、同様にして、ファイル鍵から認証情報を生成し、生成した認証情報と暗号化ファイル鍵と対応付けて、記憶部に書き込む。ファイル復号部は、ファイル鍵と認証情報とを読み出し、ファイル鍵から認証情報を生成し、読み出した認証情報と、生成した認証情報とを比較して、ファイル鍵の改竄を検証する。また、平文についても同様である。

【００７６】（８）パスワード登録部は、鍵情報を暗号化鍵と対応付けて、記憶部内の同じファイル内に書き込むとしてもよい。また、ファイル暗号部は、図９に一例として示すように、記憶部内の同じ暗号化ファイルのヘッダ部に暗号化鍵と暗号化ファイル鍵とを書き込み、データ部に暗号文を書き込むようにしてもよい。このとき、ファイル復号部は、記憶部の暗号化鍵を読み出す代わりに、暗号化ファイルのヘッダ部から暗号化鍵を読み出すようにしてもよい。

【００７７】暗号化鍵をファイルのヘッダ部に格納することにより、ヘッダ部付きの暗号化ファイルをそのまま他の計算機に移動して、パスワードだけで復号ができる。ただし、パスワードを変更した場合には、対応するファイルのヘッダ部内の暗号化鍵をすべて更新する必要がある。また、ファイル暗号時に、必要となる暗号化鍵と鍵情報を同一の媒体に格納しておくと便利である。

【００７８】（９）ファイル暗号部は、さらに、暗号化鍵と暗号文とを対応付けて１個の暗号化ファイル内に書き込むか否かを示す指示の入力を利用者から受け付け、前記指示が対応付けて書き込むことを示す場合に、前記暗号化鍵をヘッダ部に書き込み、前記暗号文をデータ部に書き込むようにしてもよい。なお、暗号化鍵を格納しないファイルは、暗号化鍵を別途保持していない環境において、パスワードを用いたファイル復号はできない。

【００７９】（１０）パスワード登録部は、生成した前記暗号化鍵を、記憶部に代えて、前記鍵記録媒体に書き込むようにしてもよい。

２．第２の実施の形態

本発明の第２の実施の形態としてのファイル管理装置１０ｂについて説明する。

【００８０】ファイル管理装置１０ｂは、ファイル管理装置１０と同様に、コンピュータシステムであり、鍵記録媒体２０が装填される。

２．１　ファイル管理装置１０ｂ及び鍵記録媒体２０の構成

ファイル管理装置１０ｂ及び鍵記録媒体２０の構成について説明する。ファイル管理装置１０ｂは、図１０に示すように、パスワード登録部１００ｂ、ファイル暗号部

２００ｂ、ファイル復号部３００ｂ及び記憶部４００ｂから構成されており、鍵記録媒体２０が接続される。

【００８１】パスワード登録部１００ｂは、パスワード入力部１０１ｂ及び暗号化部１０２ｂから構成され、ファイル暗号部２００ｂは、ファイル鍵生成部２０１ｂ、暗号化部２０２ｂ、暗号化部２０３ｂ、暗号化部２０４ｂ及び復号部２０５ｂから構成され、ファイル復号部３００ｂは、パスワード入力部３０１ｂ、復号部３０２ｂ、切換部３０３ｂ、復号部３０４ｂ及び復号部３０５ｂから構成される。

【００８２】以下において、ファイル管理装置１０の構成部との相違点を中心として説明する。

（１）記憶部４００ｂ

記憶部４００ｂは、記憶部４００と同様であり、あらかじめ、平文を含む平文ファイル４０１ｂを記憶している。

【００８３】（２）パスワード入力部１０１ｂ

パスワード入力部１０１ｂは、パスワード入力部１０１と同様に、入力を受け付けたパスワードを暗号化部１０２ｂへ出力する。

（３）暗号化部１０２ｂ

暗号化部１０２ｂは、暗号化部１０２と同様であり、鍵記録媒体２０から読み出した鍵情報を鍵として用いて、パスワード入力部１０１ｂから受け取ったパスワードに暗号アルゴリズムＥ１を施して、暗号化パスワードを生成し、生成した暗号化パスワードを１個のファイルとして記憶部４００ｂ内に書き込む。

【００８４】（４）ファイル鍵生成部２０１ｂ

ファイル鍵生成部２０１ｂは、ファイル鍵生成部２０１と同様に、ファイル鍵を生成し、生成したファイル鍵を暗号化部２０２ｂ、暗号化部２０３ｂ及び暗号化部２０４ｂへ出力する。

（５）復号部２０５ｂ

復号部２０５ｂは、記憶部４００ｂに記憶されている暗号化パスワードを読み出し、鍵記録媒体２０から鍵情報を読み出す。次に、読み出した前記鍵情報を用いて、読み出した前記暗号化パスワードに復号アルゴリズムＤ１を施してパスワードを生成し、生成したパスワードを暗号化部２０２ｂへ出力する。

【００８５】（６）暗号化部２０３ｂ

暗号化部２０３ｂは、暗号化部２０３と同様であり、記憶部４００ｂから平文ファイル４０１ｂを読み出し、ファイル鍵生成部２０１ｂからファイル鍵を受け取る。次に、暗号化部２０３は、受け取ったファイル鍵を鍵として用いて、平文ファイル４０１ｂ内に含まれる平文に暗号アルゴリズムＥ３を施して暗号文を生成し、データ部内に生成した前記暗号文を含む暗号化ファイル４０４ｂを記憶部４００に書き込む。

【００８６】（７）暗号化部２０２ｂ

暗号化部２０２ｂは、復号部２０５ｂからパスワードを

受け取り、ファイル鍵生成部２０１ｂからファイル鍵を受け取る。次に、受け取ったパスワードを鍵として用いて、受け取ったファイル鍵に暗号アルゴリズムＥ２を施して第１暗号化ファイル鍵を生成し、生成した前記第１暗号化ファイル鍵を、記憶部４００ｂの暗号化ファイル４０４ｂ内のヘッダ部内に書き込む。

【００８７】（８）暗号化部２０４ｂ

暗号化部２０４ｂは、鍵記録媒体２０から鍵情報を読み出し、ファイル鍵生成部２０１ｂからファイル鍵を受け取る。次に、暗号化部２０４ｂは、読み出した鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムＥ４を施して第２暗号化ファイル鍵を生成し、生成した前記第２暗号化ファイル鍵を、記憶部４００ｂの暗号化ファイル４０４ｂ内のヘッダ部内に書き込む。ここで、暗号アルゴリズムＥ４は、ＤＥＳによるものである。

【００８８】（９）切換部３０３ｂ

切換部３０３ｂは、利用者から第１及び第２タイプのいずれかの入力を受け付ける。第１タイプは、パスワードを用いて暗号文を復号することを示し、第２タイプは、鍵情報を用いて暗号文を復号することを示す。切換部３０３ｂは、第１タイプの入力を受け付けた場合には、復号部３０２ｂからファイル鍵を受け取り、受け取った前記ファイル鍵を復号部３０５ｂへ出力する。第２タイプの入力を受け付けた場合には、復号部３０４ｂからファイル鍵を受け取り、受け取った前記ファイル鍵を復号部３０５ｂへ出力する。

【００８９】（１０）パスワード入力部３０１ｂ

パスワード入力部３０１ｂは、パスワード入力部１０１と同様に、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部３０２ｂへ出力する。

（１１）復号部３０２ｂ

復号部３０２ｂは、パスワード入力部３０１ｂからパスワードを受け取り、記憶部４００ｂの暗号化ファイル４０４ｂのヘッダ部に含まれる第１暗号化ファイル鍵を読み出す。読み出したパスワードを鍵として用いて、読み出した前記第１暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵情報を生成し、生成したファイル鍵を切換部３０３ｂへ出力する。

【００９０】（１１）復号部３０４ｂ

復号部３０４ｂは、鍵記録媒体２０から鍵情報を読み出し、記憶部４００ｂの暗号化ファイル４０４のヘッダ部に含まれる第２暗号化ファイル鍵を読み出し、読み出した前記鍵情報を鍵として用いて、読み出した第２暗号化ファイル鍵に復号アルゴリズムＤ４を施してファイル鍵を生成する。ここで、復号アルゴリズムＤ４は、ＤＥＳによるものであり、暗号アルゴリズムＥ４の逆変換を行うアルゴリズムである。

【００９１】次に、復号部３０４は、生成したファイル鍵を切換部３０３ｂへ出力する。

（１２）復号部３０５ｂ

復号部３０５ｂは、復号部３０４ｂからファイル鍵を受け取り、記憶部４００ｂから暗号化ファイル４０４ｂのデータ部に含まれる暗号文を読み出し、受け取った前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成する。次に、復号部３０５ｂは、生成した前記復号文を含む復号文ファイル４０２ｂを記憶部４００内に書き込む。

【００９２】２．２　ファイル管理装置１０ｂの動作

ファイル管理装置１０ｂの動作について説明する。

（１）パスワード登録部１００ｂの動作

パスワード登録部１００ｂの動作について、図１１に示すフローチャートを用いて説明する。

【００９３】パスワード入力部１０１ｂは、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを暗号化部１０２ｂへ出力する（ステップＳ２０１）。次に、暗号化部１０２ｂは、鍵記録媒体２０の記憶領域から鍵情報を読み出し（ステップＳ２０２）、前記鍵情報を鍵として用いて、前記パスワードに暗号アルゴリズムＥ１を施して、暗号化パスワードを生成し（ステップＳ２０３）、生成した前記暗号化パスワードを１個のファイルとして記憶部４００ｂ内に書き込む（ステップＳ２０４）。

【００９４】（２）ファイル暗号部２００ｂの動作

ファイル暗号部２００ｂの動作について、図１２に示すフローチャートを用いて説明する。復号部２０５ｂは、記憶部４００ｂに記憶されている暗号化パスワードを読み出し、鍵記録媒体２０から鍵情報を読み出し、読み出した前記鍵情報を用いて、読み出した前記暗号化パスワードに復号アルゴリズムＤ１を施してパスワードを生成し、生成したパスワードを暗号化部２０２ｂへ出力する（ステップＳ２２１）。

【００９５】次に、ファイル鍵生成部２０１ｂは、ファイル鍵を生成する（ステップＳ２２２）。次に、暗号化部２０３ｂは、平文ファイル４０１ｂを記憶部４００ｂから読み出し、ファイル鍵を鍵として用いて、平文ファイル４０１ｂ内に含まれる平文に暗号アルゴリズムＥ３を施して暗号文を生成し（ステップＳ２２３）、データ部内に生成した前記暗号文を含む暗号化ファイル４０４ｂを記憶部４００ｂに書き込む（ステップＳ２２４）。

【００９６】次に、暗号化部２０２ｂは、パスワードとファイルとを受け取り、パスワードを鍵として用いて、前記ファイル鍵に暗号アルゴリズムＥ２を施して第１暗号化ファイル鍵を生成し、（ステップＳ２２５）、生成した前記第１暗号化ファイル鍵を、記憶部４００ｂの暗号化ファイル４０４ｂ内のヘッダ部内に書き込む（ステップＳ２２６）。

【００９７】次に、暗号化部２０４ｂは、ファイル鍵と鍵情報とを受け取り、鍵情報を鍵として用いて、前記ファイル鍵に暗号アルゴリズムＥ４を施して第２暗号化ファイル鍵を生成し、（ステップＳ２２７）、生成した前記第２暗号化ファイル鍵を、記憶部４００ｂの暗号化ファイル４０４ｂ内のヘッダ部内に書き込む（ステップＳ２２８）。

【００９８】（３）ファイル復号部３００ｂの動作

ファイル復号部３００ｂの動作について、図１３に示すフローチャートを用いて説明する。切換部３０３ｂは、利用者から第１及び第２タイプのいずれかの入力を受け付ける（ステップＳ２４１）。

【００９９】切換部３０３ｂが第１タイプの入力を受け付けた場合には、（ステップＳ２４２）、パスワード入力部３０１ｂは、利用者からパスワードの入力を受け付け、受け付けた前記パスワードを復号部３０２ｂへ出力し（ステップＳ２４５）、復号部３０２ｂは、記憶部４００ｂから第１暗号化ファイル鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記第１暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成し、前記ファイル鍵を切換部３０３ｂを介して復号部３０５ｂへ出力する（ステップＳ２４６）。

【０１００】切換部３０３ｂが第２タイプの入力を受け付けた場合には（ステップＳ２４２）、復号部３０４ｂは、鍵記録媒体２０から鍵情報を読み出し（ステップＳ２４３）、記憶部４００ｂから第２暗号化ファイル鍵を読み出し、前記鍵情報を鍵として用いて、読み出した前記第２暗号化ファイル鍵に復号アルゴリズムＤ４を施してファイル鍵を生成し、前記ファイル鍵を切換部３０３ｂを介して復号部３０５ｂへ出力する（ステップＳ２４４）。

【０１０１】次に、復号部３０５ｂは、記憶部４００ｂから暗号化ファイル４０４ｂのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成し（ステップＳ２４７）、次に、復号部３０５ｂは、生成した前記復号文を含む復号文ファイル４０２ｂを記憶部４００ｂ内に書き込む（ステップＳ２４８）。

【０１０２】２．３　まとめ

ファイル管理装置１０ｂは、パスワードの登録、平文の暗号化及び暗号文の復号の３つの部分を含んでいる。パスワードの登録時には、利用者は、鍵情報の記録されている鍵記録媒体を装填し、登録するパスワードを入力する。パスワード登録部１００ｂは、鍵情報を用いて入力されたパスワードを暗号化し、生成された暗号化パスワードをコンピュータシステム内に保存する。第１の実施の形態と比較すると、暗号化の対象となる情報と、暗号化の際に用いられる鍵とが、逆になっている。

【０１０３】次に、ファイルの暗号時には、利用者は前記暗号化パスワードの存在するコンピュータシステム内において、鍵記録媒体を装填し、暗号化するファイルを指定する。ファイル暗号部２００ｂは、まず前記暗号化パスワードを鍵情報で復号して、パスワードを求める。次に、任意に生成したファイル鍵をこのパスワードを用

いて暗号化して第１暗号化ファイル鍵を生成する。また、鍵情報を用いてファイル鍵を暗号化して第２暗号化ファイル鍵を生成する。さらにファイル鍵でファイルの情報を暗号化して暗号文を生成し、そして第１及び第２暗号化ファイル鍵をヘッダ部に、暗号文をデータ部に含む暗号化ファイルを記憶部に書き込む。

【０１０４】暗号化ファイルの復号には、パスワードを用いる方法と鍵情報を用いる方法とがある。ファイル復号部３００ｂは、鍵情報を用いる場合には、暗号化ファイルのヘッダ部から獲得した第２暗号化ファイル鍵を鍵情報を用いて復号し、ファイル鍵を求め、次に、暗号文をそのファイル鍵で復号する。パスワードを用いる場合には、利用者からパスワードの入力を受け付け、第１暗号化ファイル鍵をパスワードを用いて復号してファイル鍵を求め、次に暗号文をそのファイル鍵で復号してもとの平文を求める。

【０１０５】２．４　変形例

ファイル管理装置１０ｂは、次に示すように構成してもよい。

（１）パスワード登録部１００ｂは、前記利用者ＩＤの入力を受け付け、暗号化パスワードを、特定のコンピュータシステムの中で、利用者ＩＤと対応させて保存しておいてもよい。このとき、ファイル暗号部２００ｂは、さらに前記利用者ＩＤの入力を受け付け、入力された前記利用者ＩＤに対応付けられた前記暗号化パスワードを復号する。

【０１０６】（２）パスワードを変更する場合の動作について、図１４に示すフローチャートを用いて説明する。パスワード登録部１００ｂは、鍵記録媒体２０から鍵情報を読み出し、暗号化ファイル４０４ｂから第２暗号化ファイル鍵を読み出し、前記鍵情報を鍵として用いて第２暗号化ファイル鍵に復号アルゴリズムＤ４を施してファイル鍵を生成する（ステップＳ２６１）。次に、パスワード登録部１００ｂは、新たなパスワードの入力を受け付け（ステップＳ２６２）、新たなパスワードを用いてファイル鍵に暗号アルゴリズムＥ２を施して新第１暗号化ファイル鍵を生成し（ステップＳ２６３）、次に、新第１暗号化ファイル鍵を暗号化ファイル４０４ｂ内の第１暗号化ファイル鍵に上書きする（ステップＳ２６４）。

【０１０７】（３）パスワードによる暗号文の復号を禁止する場合には、ファイル管理装置１０ｂは、暗号化ファイル４０４ｂ内の第１暗号化ファイル鍵を削除する。このとき、鍵情報を用いた暗号文の復号は可能である。

（４）鍵情報を変更する場合の動作について、図１５に示すフローチャートを用いて説明する。

【０１０８】前記鍵記録媒体は、前記鍵情報（旧鍵情報と呼ぶ）に代えて、新たな鍵情報（新鍵情報と呼ぶ）を予め記憶している。ファイル暗号部２００ｂは、前に入力されたものものと同じパスワードの入力を受け付け

（ステップＳ２８１）、暗号化ファイル４０４ｂから第１暗号化ファイル鍵を読み出し（ステップＳ２８２）、前記パスワードを鍵として用いて、第１暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成する（ステップＳ２８３）。次に、ファイル暗号部２００ｂは、鍵記憶媒体から新鍵情報を読み出し、新鍵情報を鍵として用いてファイル鍵に暗号アルゴリズムＥ４を施して新第２暗号化ファイル鍵を生成し（ステップＳ２８４）、新第２暗号化ファイル鍵を暗号化ファイル４０４ｂ内の第２暗号化ファイル鍵に上書きする（ステップＳ２８５）。

【０１０９】（５）上記の実施の形態では、暗号化パスワードは、１個のコンピュータシステム内に保存しているので、パスワードによる暗号文の復号は、当該コンピュータシステム内でのみ可能となる。ここで、他のコンピュータシステムにおいて、パスワードによる復号を可能にするためには、暗号化パスワードを可搬型の別記録媒体に格納し、他のコンピュータシステムに入力すればよい。

【０１１０】ここで、１個のコンピュータシステムのパスワード登録部は、ＳＤメモリカードなどの可搬型の記録媒体に暗号化パスワードを書き込む。また、利用者は、暗号化ファイルを可搬型の記録媒体に書き込む。次に、利用者は、暗号化パスワードの書き込まれた記録媒体と、暗号化ファイルの書き込まれた記録媒体を他のコンピュータシステムに装填し、他のコンピュータシステムが備えるファイル復号部は、可搬型記録媒体から暗号化パスワードを読み出し、復号し、また可搬型記録媒体から暗号文を読み出し、復号する。

【０１１１】ここで、暗号化パスワードと暗号文とを１個のファイルとして、１個の可搬型の記録媒体に書き込むとしてもよい。

（６）平文を暗号化して暗号文を生成するときに、暗号化ファイルのヘッダ部に暗号化の有無や対応する鍵情報の利用者ＩＤを格納し、鍵情報やパスワードが更新されたときに、上記（２）又は（４）の手順において、これら暗号化の有無や利用者ＩＤなどの情報を用いて、暗号化ファイルを検索するようにしてもよい。また、各暗号化ファイルのヘッダ部内にこれらの情報を書き込む代わりに、暗号化ファイル毎に、これらの情報を一括して一括ファイルに書き込んでおいて、一括ファイルを用いて、暗号化ファイルを検索するようにしてもよい。

【０１１２】（７）平文を暗号化して暗号文を生成するときに、利用者からの指示を受け付けて、指示の内容によって、暗号化ファイルのヘッダ部内に第１暗号化ファイル鍵を格納するか否かを選択するようにしてもよい。第１暗号化ファイル鍵を格納することが選択された場合には、上記と同様にして第１暗号化ファイル鍵を暗号化ファイルのヘッダ部内に格納する。格納しないことが選択された場合には、第１暗号化ファイル鍵の生成と、第

１暗号化ファイル鍵の格納とを行わない。第１暗号化ファイル鍵を格納する場合には、パスワードによる暗号文の復号が可能である。格納しない場合には、パスワードによる復号が禁止できる。

【０１１３】（８）利用者が鍵情報を紛失した場合に、鍵情報による暗号文の復号を禁止するときに、ファイル管理装置１０ｂは、第２暗号化ファイル鍵を削除する。これにより、紛失した鍵情報を不正者が入手して復号することを禁止でき、第２の実施の形態では、第１の実施の形態で不可能であった、鍵情報を紛失したときの当該鍵情報の一時無効化を可能にしている。このとき、パスワードを用いた暗号文の復号は可能である。

【０１１４】さらに、（４）に示す構成より、パスワードによる復号は可能である。こうして、新しい鍵情報が発行されるまで利用者本人は不自由なくファイルにアクセスできる。また新しい鍵情報が再発行された場合には、暗号化ファイルのヘッダ部を更新するだけで、新しい鍵情報を用いて、以降は復号できるようにできる。以下において、図１６～図１８に示すフローチャートを用いて、利用者が鍵記録媒体を紛失した場合の処理について、説明する。

【０１１５】これらのフローチャートに示すように、利用者が鍵記録媒体を紛失した場合には、鍵情報の一時無効化処理がなされる（ステップＳ３０１）。次に、鍵情報が一時無効化されている期間において、利用者が暗号文を復号するときには、パスワードによる復号処理がなされる（ステップＳ３０２）。次に、新鍵情報が発行され、新鍵情報を記録している鍵記録媒体が利用者に新たに提供された場合には、新第２暗号化ファイルを生成し（ステップＳ３０３）、新鍵情報を用いて通常の復号処理が行われる（ステップＳ３０４）。

【０１１６】次に、ステップＳ３０１～Ｓ３０４の詳細について説明する。ステップＳ３０１における鍵情報の一時無効化処理において、ファイル管理装置１０ｂは、第２暗号化ファイル鍵を削除する（ステップＳ３１１）。ステップＳ３０２におけるパスワードによる復号処理において、パスワード入力部３０１ｂは、利用者からパスワードの入力を受け付け（ステップＳ３２１）、復号部３０２ｂは、記憶部４００ｂから第１暗号化ファイル鍵を読み出し、前記パスワードを鍵として用いて、読み出した前記第１暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成し、前記ファイル鍵を切換部３０３ｂを介して復号部３０５ｂへ出力する（ステップＳ３２２）。次に、復号部３０５ｂは、記憶部４００ｂから暗号化ファイル４０４ｂのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成し（ステップＳ３２３）、次に、復号部３０５ｂは、生成した前記復号文を含む復号文ファイル４０２ｂを記憶部４００ｂ内に書き込む（ステップＳ３２４）。

【０１１７】ステップＳ３０３における新第２暗号化ファイルを生成処理において、ファイル暗号部２００ｂは、前に入力されたものものと同じパスワードの入力を受け付け（ステップＳ３３１）、暗号化ファイル４０４ｂから第１暗号化ファイル鍵を読み出し（ステップＳ３３２）、前記パスワードを鍵として用いて、第１暗号化ファイル鍵に復号アルゴリズムＤ２を施してファイル鍵を生成する（ステップＳ３３３）。次に、ファイル暗号部２００ｂは、鍵記憶媒体から新鍵情報を読み出し、新鍵情報を鍵として用いてファイル鍵に暗号アルゴリズムＥ４を施して新第２暗号化ファイル鍵を生成し（ステップＳ３３４）、新第２暗号化ファイル鍵を暗号化ファイル４０４ｂ内の第２暗号化ファイル鍵に上書きする（ステップＳ３３５）。

【０１１８】ステップＳ３０４における新鍵情報を用いる通常の復号処理において、復号部３０４ｂは、鍵記録媒体から新鍵情報を読み出し（ステップＳ３４１）、記憶部４００ｂから新第２暗号化ファイル鍵を読み出し、前記新鍵情報を鍵として用いて、読み出した前記新第２暗号化ファイル鍵に復号アルゴリズムＤ４を施してファイル鍵を生成し、前記ファイル鍵を切換部３０３ｂを介して復号部３０５ｂへ出力する（ステップＳ３４２）。次に、復号部３０５ｂは、記憶部４００ｂから暗号化ファイル４０４ｂのデータ部に含まれる暗号文を読み出し、前記ファイル鍵を鍵として用いて、読み出した暗号文に復号アルゴリズムＤ３を施して復号文を生成し（ステップＳ３４３）、次に、復号部３０５ｂは、生成した前記復号文を含む復号文ファイル４０２ｂを記憶部４００ｂ内に書き込む（ステップＳ３４４）。

【０１１９】（９）ファイル復号部３００ｂは、暗号文の復号時に、鍵情報及びパスワードの両方要求するようにしてもよい。また、第１及び第２暗号化ファイル鍵をそれぞれパスワード及び鍵情報を用いて復号して、２個のファイル鍵を生成し、生成された２個のファイル鍵が一致するか否かを判断することにより、暗号化ファイルのヘッダ部の改竄を検出するようにしてもよい。

【０１２０】（１０）第１の実施の形態の変形例と同様に、暗号化パスワード、第１暗号化ファイル鍵、第２暗号化ファイル鍵、暗号文に、認証情報を付加し、認証情報を用いて、これらの情報の改竄を検出するようにしてもよい。

３．まとめ

以上のように本発明によれば、計算機に付随した鍵情報を用いてファイルの暗号化と復号とが可能になる。加えて、暗号時に指定すれば復号時に鍵情報無しで、あらかじめ登録して計算機内に安全に保管しておいたパスワードを用いて復号が可能になる。ファイル暗号時には逐次パスワードを設定する必要はない。また、利用者がパスワードを忘却したときにパスワードによる復号を一時的

に無効化したり、新しいパスワードに容易に変更できる仕組みを備える。さらに、鍵情報を紛失したときに、鍵情報を一時的に無効化したり、新しい鍵情報が発行されたときにも、ヘッダ部だけを更新することにより、新しい鍵情報で前の鍵情報で暗号化したファイルを扱えるための仕組みを備える。また、鍵情報やパスワードのIDをヘッダや一括管理ファイルに格納することにより、鍵情報やパスワードの変更時にそれに伴う変更が可能である暗号化ファイルを検索することができる。

【０１２１】こうして、本発明では次の条件を満たすファイル暗号復号システムを提供することができる。

（１）ICカードのような記録媒体に格納した鍵情報を用いてファイルの暗号化を行なう。パスワードはあらかじめ登録しておき、逐一のパスワード入力は必要ないものとする。

【０１２２】（２）前記鍵情報を用いてファイルの復号ができる。また、暗号化したときの指定によりあらかじめ登録したパスワードを用いたファイルの復号も可能とする。

（３）パスワードを容易に変更できる仕組みを備える。

（４）前記鍵情報を紛失した場合に、一時的に鍵情報を無効化する仕組みを備える。さらに、新しい鍵情報が再発行された場合に、新しい鍵情報で以前のファイルが取り扱えるための仕組みを備える。また、そのために変更すべき暗号化ファイルを容易に検索する仕組みを備える。

【０１２３】４．その他の変形例

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

（１）上記の実施の形態において、暗号及び復号アルゴリズムとしてＤＥＳを用いるとしているが、他の暗号及び復号アルゴリズムを用いてもよい。

【０１２４】（２）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、フロッピー（登録商標）ディスク、ハードディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤ、ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【０１２５】また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【０１２６】また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

（３）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【０１２７】

【発明の効果】上記の目的を達成するために、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、入力されるパスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成する登録手段と、前記鍵記録媒体に記憶されている鍵情報に基づいて、平文を暗号化して暗号文を生成する暗号手段と、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換える切換手段と、前記鍵情報に基づいて暗号文を復号する復号手段とを備える。また、前記ファイル管理装置は、さらにメモリ部を有し、前記登録手段は、パスワードの入力を受け付け、前記パスワードを用いて前記鍵情報を暗号化して暗号化鍵を生成し、生成した前記暗号化鍵をメモリ部に書き込み、前記暗号手段は、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して暗号化ファイル鍵を生成し、前記暗号文と前記暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記暗号化鍵を復号して鍵情報を生成する第１鍵獲得手段と、第２タイプの入力を受け付けた場合に、前記鍵記録媒体から鍵情報を読み出す第２鍵獲得手段とを含み、前記切換手段は、前記第１及び第２鍵獲得手段のいずれかにより鍵情報を獲得し、前記復号手段は、前記鍵情報を用いて前記暗号化ファイル鍵を復号してファイル鍵を生成し、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【０１２８】この構成によると、前記鍵記録媒体から鍵情報を読み出すか、又は入力されるパスワードを用いて前記暗号化鍵を復号して鍵情報を生成するかを切り換え、前記鍵情報に基づいて暗号文を復号するので、パスワードによらずとも復号することができる。また、本発明は、平文を暗号化して記憶し、復号するファイル管理装置であって、鍵情報を予め記憶している鍵記録媒体と、前記鍵情報を用いて入力されるパスワードを暗号化する登録手段と、ファイル鍵を用いて平文を暗号化して

暗号文を生成し、前記鍵情報と前記暗号化されたパスワードを復号して得られたパスワードとに基づいて、ファイル鍵を暗号化してそれぞれ暗号化ファイル鍵を生成する暗号手段と、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成する切換手段と、前記ファイル鍵に基づいて暗号文を復号する復号手段とを備える。また、前記ファイル管理装置は、平文を暗号化してメモリ部に記憶し、前記登録手段は、パスワードの入力を受け付け、前記鍵情報を用いて前記パスワードを暗号化して暗号化パスワードを生成し、生成した前記暗号化パスワードをメモリ部に書き込み、前記暗号手段は、前記鍵情報を用いて前記暗号化パスワードを復号してパスワードを生成し、ファイル鍵を用いて平文を暗号化して暗号文を生成し、前記パスワードを用いて前記ファイル鍵を暗号化して第１暗号化ファイル鍵を生成し、前記鍵情報を用いて前記ファイル鍵を暗号化して第２暗号化ファイル鍵を生成し、前記暗号文と前記第１及び第２暗号化ファイル鍵とを対応付けてメモリ部に書き込み、前記切換手段は、前記パスワードの入力を受け付け、前記パスワードを用いて前記第１暗号化ファイル鍵を復号してファイル鍵を生成する第１鍵獲得手段と、前記鍵記録媒体に記憶されている鍵情報を用いて前記第２暗号化ファイル鍵を復号してファイル鍵を生成する第２鍵獲得手段とを含み、前記第１及び第２鍵獲得手段のいずれかによりファイル鍵を獲得し、前記復号手段は、前記ファイル鍵を用いて前記暗号文を復号して復号文を生成するように構成してもよい。

【０１２９】この構成によると、前記鍵情報に基づいて暗号化ファイル鍵を復号するか、又は入力されたパスワードに基づいて暗号化ファイル鍵を復号するかを切り換えて、ファイル鍵を生成し、前記ファイル鍵に基づいて暗号文を復号するので、パスワードによらずとも復号することができる。

【図面の簡単な説明】

【図１】第１の実施の形態としてのファイル管理装置１０の外観を示す。

【図２】ファイル管理装置１０の構成を示すブロック図である。

【図３】パスワード登録部１００の動作を示すフローチャートである。

【図４】ファイル暗号部２００の動作を示すフローチャートである。

【図５】ファイル復号部３００の動作を示すフローチャートである。

【図６】利用者ＩＤテーブルの一例を示す。

【図７】パスワードを変更する場合のファイル管理装置の動作を示すフローチャートである。

【図８】鍵情報を更新する場合のファイル管理装置の動作を示すフローチャートである。

【図９】暗号化ファイルのデータ構造の一例を示す。

【図１０】第２の実施の形態としてのファイル管理装置１０ｂの構成を示すブロック図である。

【図１１】パスワード登録部１００ｂの動作を示すフローチャートである。

【図１２】ファイル暗号部２００ｂの動作を示すフローチャートである。

【図１３】ファイル復号部３００ｂの動作を示すフローチャートである。

【図１４】パスワードを変更する場合の動作を示すフローチャートである。

【図１５】鍵情報を変更する場合の動作を示すフローチャートである。

【図１６】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図１７へ続く。

【図１７】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図１８へ続く。

【図１８】鍵記録媒体を紛失した場合の動作を示すフローチャートである。図１７から続く。

【符号の説明】

１０　ファイル管理装置
１０ｂ　ファイル管理装置
２０　鍵記録媒体
１００　パスワード登録部
１００ｂ　パスワード登録部
１０１　パスワード入力部
１０１ｂ　パスワード入力部
１０２　暗号化部
１０２ｂ　暗号化部
２００　ファイル暗号部
２００ｂ　ファイル暗号部
２０１　ファイル鍵生成部
２０１ｂ　ファイル鍵生成部
２０２　暗号化部
２０２ｂ　暗号化部
２０３　暗号化部
２０３ｂ　暗号化部
２０４ｂ　暗号化部
２０５ｂ　復号部
３００　ファイル復号部
３００ｂ　ファイル復号部
３０１　パスワード入力部
３０１ｂ　パスワード入力部
３０２　復号部
３０２ｂ　復号部
３０３　切換部
３０３ｂ　切換部
３０４　復号部
３０４ｂ　復号部
３０５　復号部

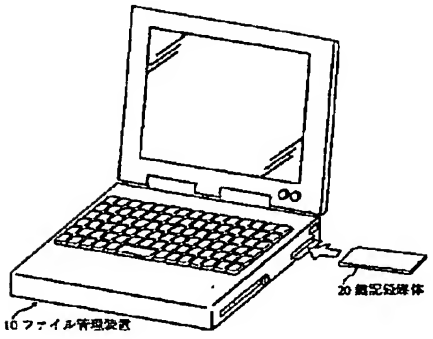
37

３０５ｂ 復号部
４００ 記憶部

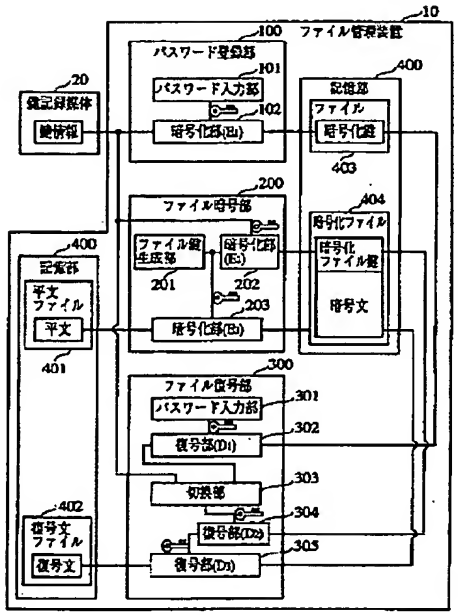
38

４００ｂ 記憶部

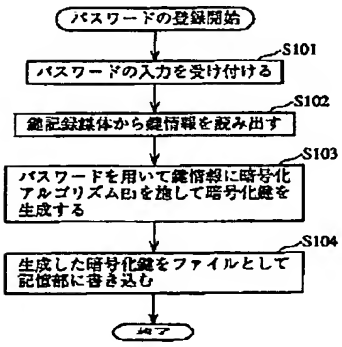
【図１】



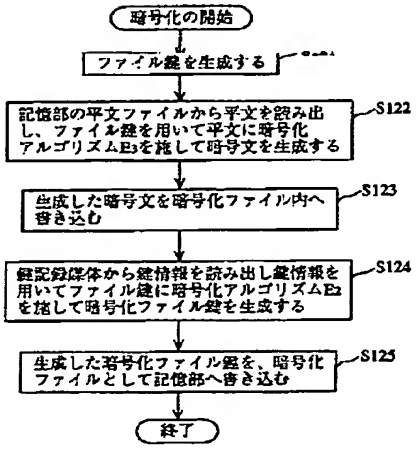
【図２】



【図３】



【図４】

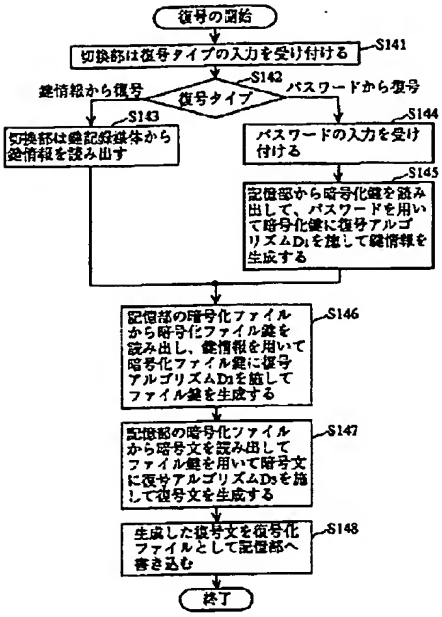


【図６】

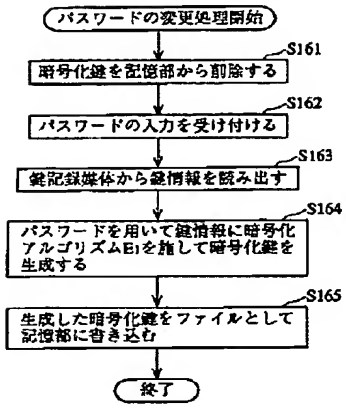
利用者IDテーブル

利用者ID	暗号化鍵
user 1	利用者1用暗号化鍵
user 2	利用者2用暗号化鍵
⋮	⋮

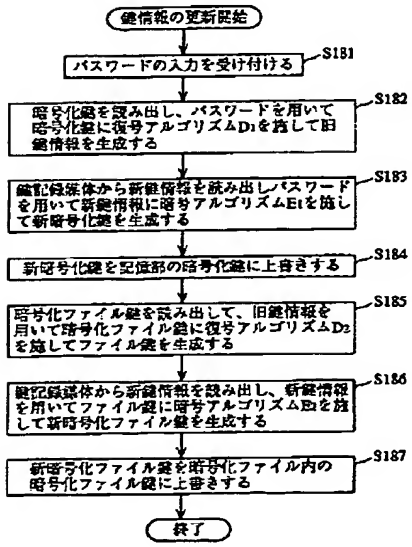
【図５】



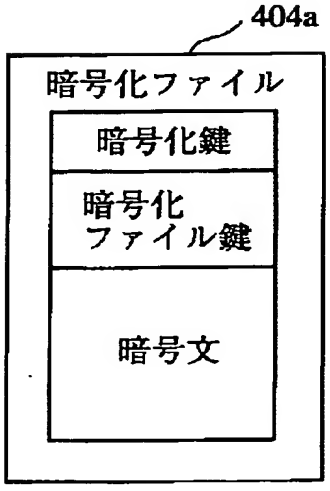
【図７】



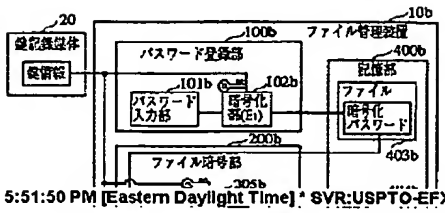
【図８】



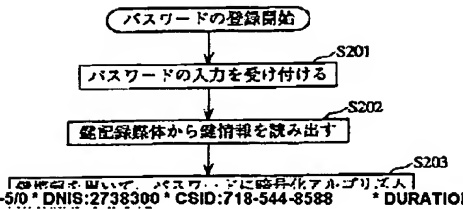
【図９】



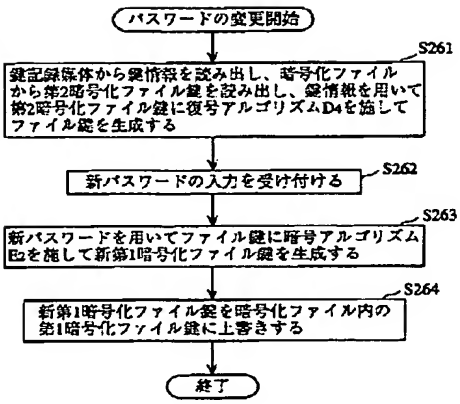
【図１０】



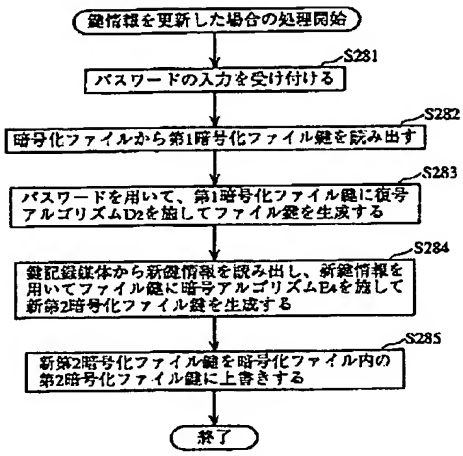
【図１１】



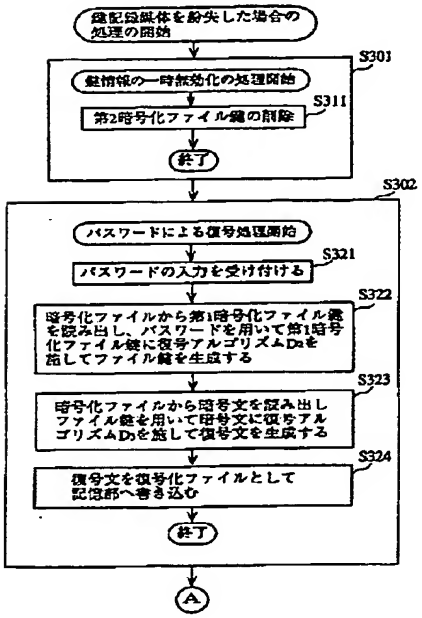
【図１４】



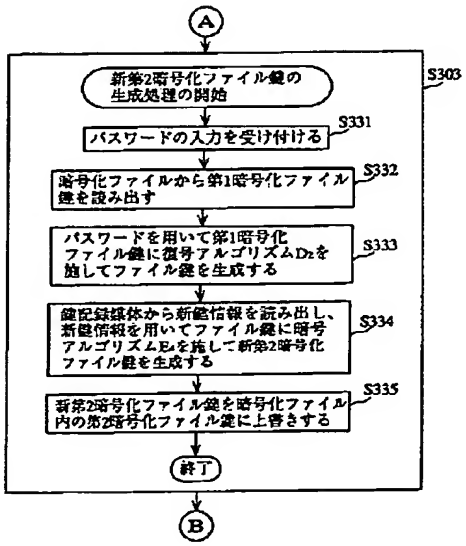
【図１５】



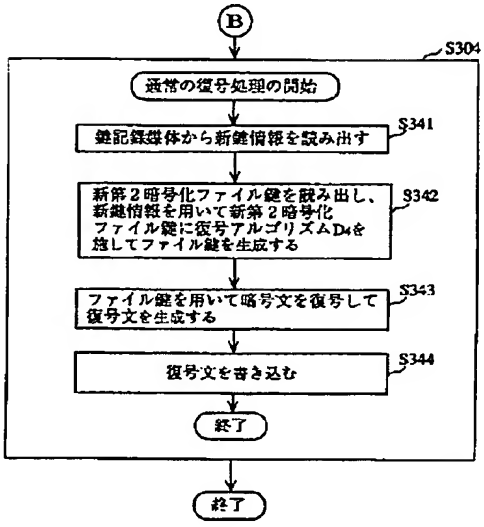
【図１６】



【図１７】



【図１８】



フロントページの続き

(51) Int. Cl.[7]	識別記号	FI	テーマコード（参考）
H04L 9/32		H04L 9/00	601C

(72) 発明者 稲垣 悟
大阪府門真市大字門真1006番地 松下電器産業 株式会社内

Fターム（参考） 5B017 AA03 BA07 CA16
5B082 EA11 GA11
5J104 AA16 EA03 EA04 EA11 EA26 JA13 NA02 NA05 NA12 NA35 NA37